CYBERRISKS&LIABILITIES

Cyberespionage Explained

Cyberespionage is a type of cyberattack that involves an unauthorized user (or multiple users) accessing a victim's sensitive information in order to secure economic benefits, competitive advantages or political gain. Also known as cyberspying, the primary targets of such cyberattacks include government entities, large corporations and other competitive organizations.

Cybercriminals may leverage cyberespionage in attempts to gather classified data, trade secrets or intellectual property (IP) from their victims. From there, cybercriminals may sell this information for profit, expose it to other parties, or use it in conjunction with military operations, potentially threatening their targets' reputations and overall stability. Oftentimes, cyberespionage is deployed across international borders by nation-state attackers.

Over the past few years, cyberespionage has become a rising concern, especially in certain countries. In fact, the FBI recently reported that the United States is currently facing cyberespionage threats from China that are "unprecedented in history." The FBI confirmed that through advanced malware programs and hacking software, the Chinese government has targeted nearly every sector of the U.S. economy and stolen more personal and corporate data from Americans than every other country combined.

With this in mind, it's crucial for businesses to understand cyberespionage and know how to effectively mitigate such incidents. This article provides a detailed overview of cyberespionage, outlines real-world examples of these cyberattacks and offers key prevention measures that businesses can implement to safeguard their operations.

Cyberespionage Overview

Although cyberespionage often involves nation-state attackers, it's not interchangeable with cyberwarfare. While cyberwarfare is conducted with the intention of noticeably disrupting a target's operations or activities, the goal of cyberespionage is for the perpetrator to remain undetected by their victim for as long as possible, therefore permitting them to gather maximum information. Yet, the information collected from cyberespionage efforts could be used later amid acts of cyberwarfare.

Any government or business could fall victim to cyberespionage. However, the U.S. Department of Homeland Security reported that organizations within the United States, the United Kingdom, Japan, Russia, China and South Korea are particularly vulnerable. After all, these countries possess high-income economies and advanced technological infrastructures, thus making them more attractive to cybercriminals.

When leveraging cyberespionage, perpetrators may attempt to access a wide range of data from their targets, including:

- Research and development activities
- Critical organizational projects or IP (e.g., product formulas and blueprints)
- Financial information (e.g., investment opportunities, employee salaries and bonus structures)
- Sensitive stakeholder details
- Business plans (e.g., upcoming marketing, communications or sales initiatives)
- Political strategies or military intelligence

Cybercriminals may engage in a variety of tactics to execute cyberespionage, such as:

- Exploiting security vulnerabilities in websites or browsers a target frequently visits and infecting them with malware to compromise the victim's technology (as well as any data stored on it)
- Utilizing phishing scams (i.e., deceptive emails, texts or calls) to steal login credentials and gain unsolicited privileges within a target's network
- Posing as employees or contractors and physically going to a victim's workplace to steal hard copies of data or infect devices with malware
- Bribing actual employees or contractors to share a target's sensitive information in exchange for payment
- Infiltrating another party in a victim's supply chain and using that party's digital privileges to compromise the actual target's network
- Injecting different forms of malware (e.g., Trojans and worms) within updates from third-party software applications, thus hijacking a victim's technology upon installation of these updates

In any case, cyberespionage can lead to serious consequences for impacted organizations. What's worse, as cybercriminals' tactics get more sophisticated, these incidents could become increasingly common.

Examples of Cyberespionage

Over the years, multiple large-scale cyberespionage events have occurred, including the following:

- **The Microsoft Internet Explorer incident**—Between 2009 and 2010, Chinese cybercriminals took advantage of a security vulnerability in Microsoft Internet Explorer to execute cyberespionage against at least 20 international media and technology companies, including Google, Yahoo and Adobe. Google reported that the cybercriminals, later coined the "Aurora" attackers, stole various IPs from the company and compromised many Gmail accounts.
- **The U.S. Office of Personnel Management (OPM) incident**—In 2012, Chinese cybercriminals used malware to establish a digital backdoor within the OPM's network. For several years afterward, the nation-state attackers used this backdoor to engage in cyberespionage, stealing personal information from more than 20 million Americans—namely, those who worked or applied to work for the federal government. The backdoor went undetected until 2015.
- **The Sony Pictures Entertainment (SPE) incident**—In 2014, a North Korean hacking group named the "Guardians of Peace" deployed cyberespionage against SPE during the months leading up to the entertainment company's release of a film that depicted the assassination of the nation-state's leader. The cybercriminals used malware to compromise SPE's network and publicly expose a substantial amount of sensitive company data, such as personal details about employees, email exchanges between staff, information regarding executives' salaries, copies of unreleased films and plans for future films. The incident significantly impacted the film's release and garnered attention from the U.S. government.
- **The SolarWinds incident**—In 2020, the U.S. government discovered that a Russian hacking group called "Cozy Bear" had conducted cyberespionage against several federal agencies and major organizations by infiltrating a common party within their supply chains. The hackers initially infected the technology company SolarWinds' network monitoring platform with malware before using that platform to gain access to sensitive data and confidential emails from various U.S. government departments and private organizations. The incident is estimated to have impacted over 18,000 of SolarWinds' customers.

Considering these incidents and their associated ramifications, it's clear that businesses need to take action to properly protect themselves against cyberespionage.

Cyberespionage Prevention Measures

Businesses should consider implementing the following best practices to help safeguard their operations from cyberespionage:

- **Educate employees.** Be sure employees receive training on cyberespionage and related prevention tactics. Specifically, employees should be instructed to never respond to messages from unknown senders, avoid interacting with suspicious links or attachments and refrain from sharing sensitive company information online. In addition, employees should be required to form complex and unique passwords for all workplace technology.
- **Protect critical data.** Review and update existing cybersecurity policies to ensure they promote maximum data protection. Implement new policies as needed (e.g., a Bring-Your-Own-Device policy and data breach response policy). Further, encrypt and store all critical data in safe, secure locations.
- **Restrict access.** Only permit employees to access technology and data they need to perform their job duties. Require employees to implement multifactor authentication whenever possible.
- **Leverage sufficient software**. Protect all workplace technology (and the data stored on it) with proper security software. This software may include endpoint detection tools, antivirus programs, firewalls, network monitoring services and patch management products. Review this software regularly for vulnerabilities and make adjustments when necessary.
- **Assess supply chain exposures.** Assess whether suppliers have adequate measures in place to protect against network infiltration from cybercriminals. Consider including specific cybersecurity requirements in all supplier contracts and keeping the amount of sensitive information shared with these parties to a minimum.
- **Have a plan.** Creating a cyber incident response plan can help ensure necessary protocols are in place cyberattacks occur, thus keeping related damages at a minimum. This plan should be well-documented, practiced regularly and address a range of cyberattack scenarios (including cyberespionage).
- **Purchase proper coverage.** It's critical to secure adequate insurance to help protect against losses that may arise from cyberespionage. It's best to consult a trusted insurance professional to discuss specific coverage needs.

Conclusion

Ultimately, cyberespionage is a pressing concern that businesses need to take seriously—especially as nation-state cyberthreats continue to rise. By understanding cyberespionage and implementing adequate prevention techniques, businesses can effectively safeguard themselves against these incidents and minimize associated losses.

For more risk management guidance, contact us today.